

Notice of Allowability

Application No.

10/062,621

Examiner

Ronald Baum

Applicant(s)

COPELAND, JOHN A.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 3/9/2007.
2. ☒ The allowed claim(s) is/are 1-36.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.


THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


5,27,07

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1-36 are allowed over prior art.
2. This action is in reply to applicant's correspondence of 09 March 2007.
3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
4. As per claims 1, 9, 10, 17 and 23 generally, prior art of record, Shipley, U.S. Patent 6,119,236 and Vaid et al, U.S. Patent 6,502,131 B1, fails to teach alone, or in combination, at the time of the invention, the features as discussed and remarked upon in the response of 09 March 2007 to office action of 10/2/2006.

Specifically, (as per claim 1, for example) prior art dealing with network traffic anomaly/misuse (i.e., determining unauthorized usage) detection/analysis via various signature capture/learning methodologies, is generally known to exist per se, (i.e., 'Network Traffic Anomaly Detector' use of the combination of pre-filtering of packets prior to the anomaly analysis, whereas the anomaly score is continuously updated as a function of packet stream event [i.e., flow like] characteristics; MAHONEY, M., "Network Traffic Anomaly Detection Based on Packet Bytes", ACM, 2003, FI. Institute of Technology, entire document, <http://www.cs.fit.edu/~mmahoney/paper6.pdf>), is generally known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the determination of suspicious activity (and the issuance thereof of a subsequent output) as a function of comparison of an observed flow with a pre-stored profile that relates the

particular host observed with a service associated with the flow, as stored as a profile), at the *time of the invention*, serving to patently distinguish the invention from said prior art;

“1. A method for determining unauthorized usage of a data communications network, comprising the steps of:

monitoring packet headers of packets

exchanged between

two hosts on the data communications network;

based on the packet headers, determining the existence of

a client/server (C/S) flow corresponding to

a predetermined plurality of packets

exchanged between

the two hosts that relate to a single service and

is characterized by

a predetermined C/S flow characteristic;

storing information associating

a service that is associated with

a determined C/S flow with

at least one of the hosts that is associated with

the determined C/S flow,

said service comprising

an observed service;

Art Unit: 2136

*determining if an observed service associated with a particular host is
out of profile by comparing
the service to
a prestored allowed network services profile for
the particular host; and
in response to determination that
an observed service associated with a particular host is out of profile,
providing an output indicating that
the observed service is out of profile.”*

5. Dependent claims 2-8, 11-16, 18-22 and 24-36 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

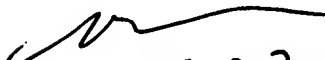
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


5,27,07

